North Carolina Banking Institute

Volume 2 | Issue 1 Article 19

1998

Electronic Banking: Security, Privacy, and CRA Compliance

Kimbrelly Kegler

Electronic Banking: Security, Privacy, and CRA Compliance

I. INTRODUCTION

In today's world of high technology and computing, consumers demand efficiency and technology in many aspects of their lives. Currently, there are over thirty-five million personal computer owners in the United States[1] and thirty million Internet users globally.[2] In addition to professional, educational, and recreational purposes, consumers are using their computers to bank online, on the world wide web, and at Internet banks. The recent history of electronic banking witnessed the creation of automated teller machine (ATM) networks in the 1960s,[3] the marketing of home financial management software programs in the 1990s, and the introduction by banks of their own proprietary home banking software in the mid to late 1990s.[4] With this software, customers

---

1. *See* Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671, 673 (1997).

2. The Internet has been described as:

> a computer network developed by the Department of Defense in the 1960s as a means to communicate with contractors and university researchers. . . . The Web, as it is frequently known, is a method of communicating and obtaining information over the Internet using 'graphical interfaces' that facilitate access to the desired information.

Steven R. England & David F. Noteware, *Banking on the Internet: Intellectual Property Pitfalls, Opportunities*, BANKING POL'Y REP., Sept. 16, 1996, at 1. Current trends indicate that by the year 2000, Internet usage will grow from 40 million to 250 million users. In addition, studies indicate that by the turn of the century over 20 million people will use Internet banking, and over 500 "full service" Internet banks will exist in the United States. *See* P. Michael Nugent, *Financial Transaction of the Internet, in* THE NEW BUSINESS OF BANKING: WHAT BANKS CAN DO NOW, at 385 (PLI Corp. Law Practice Course Handbook Series No. 966, 1996).

3. Diebold, an innovator in banking services delivery, first moved into the automated teller machine industry in the late 1960s. *See* Diebold, *Diebold - Continuing a Tradition of Quality and Leadership* (last modified May 16, 1997) <http://www.diebold.com/whoweare/index.html>.

4. *See* Charles Haddad, *New-Fashioned Banking It's Not for Everyone: Unless You're Patient or Live To Be on the Cutting Edge, An Online Checkbook Can Turn Into A Chore*, ATLANTA J. & CONST., Feb. 9, 1997, at H1 (describing Quicken, Microsoft Money, Managing Your Money, and other financial software management programs currently available to consumers).

gained the ability to conduct financial transactions from home through a modem connection to the bank.[5] As consumers became more familiar with modems and financial management software, they were also learning how to surf the Internet. Consequently, in the mid-1990s, banks started using the Internet to communicate with and attract banking customers.[6]

Initially, most bank web sites merely displayed information about their banks and the products and services they offered.[7] As Internet usage increased by banks and consumers, banks began to offer web-based banking which allows customers to transfer funds between accounts, check balances, and verify interest rates.[8] Web-based banking led to the latest progression in the history of electronic banking, the creation of true Internet banks that offer their services primarily through the Internet rather than through physical branches.[9]

In the context of this historical background, this Comment discusses the current state of electronic banking and the future of the evolving industry. More specifically, this Comment begins by discussing three forms of electronic banking.[10] Next, this Comment addresses problems associated with online and web-based banking.[11]

---

5. *See* Jon Newberry, *Anywhere, Anytime, Anyway: Online Banking Offers Greater Convenience and Easier Financial Planning*, ABA J. 94, 94 (1996); *see also* FIND/SVP, Inc., *Find/SVP Predicts 16.9 Million Online Banking Households in 2001*, ONLINE BANKING REP., May 1997, at 10 (stating that by year-end 1996, there were 2.1 million households in the United States using online banking services).

6. One commentator predicted that "18% of U.S. families will do their personal banking on the Internet. But they will represent 30% of bank profits because they will be the most educated, the most wealthy 18%." Diane Francis, *Banks Might be the Casualties in Move to Electronic Money*, FIN. POST, Feb. 11, 1997, at 21.

7. *See* Kim Yancey & Marty Fisher-Haydis, *Developments in Banking Law: 1996*, ANN. REV. BANKING L. 76, 91 (1997); FIND/SVP, Inc., *The 1997 American Internet User Survey: Online Ads are Effective* (last modified May 7, 1997) <http://etrg.findsvp.com/internet/online.html>.

8. *See, e.g.*, Bank of America, *Bank of America Homebanking Overview* (last modified Dec. 19, 1997) <http://www.bofa.com/p-finance/homebanking/homebanking.html>; First Union National Bank, *First Union Cyberbanking Center* (last modified Feb. 24, 1998) <http://www.firstunion.com/cybank.html>; NationsBank, *Welcome Home to NationsBank PC Banking* (last modified Feb. 11, 1998) <http://www.nationsbank.com/pcbanking/>; Wells Fargo, *Sign On to Online Banking* (visited Oct. 21, 1997) <http://banking.wellsfargo.com>.

9. *See, e.g.*, Atlanta Internet Bank, *Atlanta Internet Bank Home Page* (last modified Feb. 11, 1998) <http://www.atlantabank.com>; Security First Network Bank, *Security First Network Bank Lobby* (last modified July 27, 1997) <http://www.sfnb.com>.

10. *See infra* notes 14-46 and accompanying text.

11. *See infra* notes 47-83 and accompanying text.

This Comment then describes possible solutions to the problems related to electronic banking including new products and services, government legislation, and voluntary measures suggested by industry leaders.[12] Finally, this Comment concludes by discussing how the government should respond to this emerging industry and suggests possible ways to ensure that all segments of the American community can surf the wave of the future.[13]

II. ELECTRONIC BANKING

Currently, the American public uses at least three forms of electronic banking: online banking, web-based banking, and Internet banks. This section describes online banking and its limitations;[14] defines web-based banking and its advantages;[15] and explains Internet banks and their ability to take electronic banking to a new level.[16]

A. Online Banking

Online banking (or "PC banking") refers to the ability of bank customers to access their account information on a personal computer using a modem and a computer software program.[17] To access banking accounts online, PC banking customers must acquire special software from their financial institutions.[18] Once the software has been loaded on the customer's personal computer, the customer may connect her computer with the bank's server via modem to monitor account balances, pay bills online, write checks, transfer funds between accounts, or check interest rates.[19] However, the

12. *See infra* notes 84-150 and accompanying text.
13. *See infra* notes 151-55 and accompanying text.
14. *See infra* notes 17-27 and accompanying text.
15. *See infra* notes 28-32 and accompanying text.
16. *See infra* notes 33-46 and accompanying text.
17. *See* Newberry, *supra* note 5, at 94 and accompanying text.
18. *See* Security First Network Bank, *How are you different from online banking?* (last modified Feb. 9, 1998) <http://www.sfnb.com/infodesk/caq_online.html>.
19. *See* Jon Newberry, *supra* note 5, at 94; *see also* Jennifer Kingson Bloom, *Fleet Enrolling 1,000 a Day in New PC Banking Program*, AM. BANKER, Mar. 13, 1997, at 19 (stating that the Fleet Financial Group provides the common PC banking services but has added a unique option which allows its customers to transfer funds from Fleet to any

customer's account access is limited to the computer where the software is loaded.[20] The first banks to offer online banking required their customers to pay a fee for software packages that permitted the customer to connect with the bank.[21] By allowing their customers to bank online, banks began to realize a lower per transaction cost than for other forms of banking.[22] Thus many banks have minimized or even waived online banking fees to encourage customers' use of online services.[23]

Although online banking appears to provide convenience at a low cost, the process still contains flaws.[24] For example, banks may update electronic account balances only at set times, potentially leaving balances incorrect between updates.[25] In addition, some creditors do not accept online bill payments.[26] Consequently, the bank's online bill paying service must produce physical paper checks to mail to some creditors.[27] As a result, customers must continue to rely on traditional paper-based methods of banking for some transactions.

---

checking account at any bank in the United States).

20. *See* Security First Network Bank, *supra* note 18; *see also* Rob Chambers, *Banks See Future Mega-Market for Online Transactions*, ATLANTA J. & CONST., Sept. 28, 1997, at G2 (claiming that managing software programs is the most expensive facet of online banking because banks must create a program unique to their services but also one that can be used with an online service provider).

21. *See* Jennifer Kingson Bloom, *Pricing Home Banking Services a Puzzle for Vacillating Bankers*, AM. BANKER, Feb. 7, 1997, at 1 (noting that prices for home banking services range from $0 to $9.95 per month without a clear mandatory standard for the pricing structure).

22. *See* AMERICA'S COMMUNITY BANKERS, THE COMMUNITY BANKER'S GUIDE TO THE INTERNET AND HOME BANKING 38 (1997). The cost per transaction for operating a branch is $1.07, $0.54 to maintain a customer service telephone line, $0.27 to run an ATM, $0.015 to provide online banking services, and $0.010 to offer web-based banking. *See id.*

23. *See id.; see also* Leigh Gregg, *The Future of Fees for On-Line Services*, CRUNEXEC, Sept. 19, 1997, at 36 (indicating that banks are charging lower fees or are waiving fees for online banking in order to keep their customers and encourage them to change their expensive transaction habits).

24. *See* Raymond E. Muth, *Becoming Internet Access Provider Expands Horizons for Apollo Trust*, J. OF RETAIL BANKING SERV., Mar. 22, 1997, at 11.

25. *See id.* This problem, however, is not unique to online banking. For example, if a customer makes a deposit at an ATM machine, a message may appear on the screen indicating that an immediate balance inquiry may not reflect that particular deposit.

26. *See* Haddad, *supra* note 4, at H1.

27. *See id.*

B. *Web-based Banking*

As some banks attempt to work out the kinks in the online banking process, other banks are turning to the Internet as a new banking medium.[28] Web-based banking providers offer services similar to those offered by banks engaged in PC banking.[29] The major advantage of web-based banking over online banking is the more flexible access medium—the Internet. With web-based banking, the customer may access accounts from any computer that has access to the Internet since all software is loaded on the bank's central computers rather than on the individual customer's computer.[30] By maintaining the software on the bank's central computers, the bank may update its software, add services, and make other technological changes without having to redistribute software to all of its customers.

In addition to eliminating the need for customers to acquire special software, web-based banking provides cost savings to banks.[31] Like online banking, a web-based bank transaction costs about one penny, whereas a teller-assisted transaction costs more than one dollar.[32] With tremendous transaction costs savings for banks and a broader access medium for customers, more banks may begin offering web-based banking services. Furthermore, as more customers become computer savvy and banks become more technologically advanced, web-based banking may become as common as drive-through tellers.

C. *Internet Banks*

Expanding on the developments in web-based banking, a few banks have taken the cost advantages of banking electronically and improving technologies to a new extreme in the form of true Internet

---

28. *See* FIND/SVP, Inc., *The 1997 American Internet User Survey-Survey Overview* (last modified May 7, 1997) <http:etrg.findsvp.com/internet/overview.html>.

29. *See supra* notes 17-27 and accompanying text.

30. *See* Security First Network Bank, *supra* note 18.

31. *See* Rick Stouffer, *Internet-Only Financial Institution Up and Running*, BUFF. NEWS, *July 29, 1997, at E1.*

32. *See supra* note 22.

banks.[33] Internet banks permit customers to open accounts, check balances, and perform the majority of their banking activities via the World Wide Web.[34] Due to savings in transaction and operating costs, these banks typically can offer these services at lower costs to customers than traditional banks.[35] In late 1997, only three fully-operational Internet banks existed in North America. These banks include Security First Network Bank (SFNB),[36] Atlanta Internet Bank (AIB),[37] and Citizens Bank of Canada.[38]

---

33. *See supra* note 10.

34. *See*, e.g., Atlanta Internet Bank, *Atlanta Internet Bank Home Page* (last modified Feb. 11, 1998) <http://www.atlantabank.com>; Security First Network Bank, *Security First Network Bank Lobby* (last modified Feb. 28, 1998) <http://www.sfnb.com>.

35. *See infra* notes 36-38.

36. *See* Security First Network Bank, *supra* note 34. In 1995, Security First Network Bank, which is chartered by the Office of Thrift Supervision (OTS) became the first bank to offer banking services primarily on the Internet. *See* Security First Network Bank, *SFNB-News Center-Quick Facts* (last modified May 15, 1997) <http://www.sfnb.com/newscenter/quickfacts.html>. Like more traditional banks, SFNB offers its customers access to accounts through checks, ATM cards, and credit cards. *See* Jennifer Kingson Bloom, *A Virtual Bank Grapples with Reality*, AM. BANKER, Aug. 19, 1996, at 10A. Before opening its bank, SFNB decided to pass all the security and functionality tests required by the OTS in order to assure its customers that their information would be secure against unauthorized access. *See* SFNB, *Office of Thrift Supervision* (last modified Feb. 9, 1998) <http://www.sfnb.com/infodesk/ bankinfo/ots.html>. These tests were conducted by security specialists who attempted to invade the SFNB computers to gain unauthorized access to account information and to confirm in writing that the SFNB system did not allow "unauthorized or undetected access to computer accounts, with reasonable certainty." *Id.*

37. *See* Atlanta Internet Bank, *supra* note 34; Jennifer Kingson Bloom, *A Second Bank is Launched Into Cyberspace*, AM. BANKER, Oct. 18, 1996, at 1. It received an independent federal charter from the OTS in July, 1997. *See* Dean Anason, *OTS Approves Spinoff of Internet-only Thrift*, AM. BANKER, July 15, 1997, at 4. Since making its presence "virtually" known, AIB has become recognized for providing its customers with some of the highest money market account interest rates in the country. *See* Atlanta Internet Bank, *Money Market* (last modified Jan. 5, 1998) <http://www.atlantabank.com/mmda.htm> (claiming to have an exceptional money market 5.5% annual interest rate for a minimum $100 balance in addition to personalized checks, monthly statements, direct deposits, and online access); *Highest Bank Yields*, THE CINCINNATI ENQUIRER, Oct. 17, 1997, at B09 (reporting that Atlanta Internet Bank's 5.5% interest rate was one of the highest annual money market yields; Security First Network Bank had the second highest yield on six month certificates of deposit at 5.9%). AIB offers customers checking accounts, certificates of deposit, and electronic bill paying options. *See* Atlanta Internet Bank, *supra* note 34.

38. *See* Citizens Bank, *Citizens Bank* (last modified Dec. 16, 1997) <http://www.citizensbank.ca>. This virtual bank's mission is to not only offer financial services to its customers, but also to make positive contributions to the social and economic environment of its local community. *See* Brad Evenson, *No Branch Offices, No Automated Teller Machines . . . It's A Virtual Bank*, CALGARY HERALD, Feb. 9, 1997, at B8. Van City Trust, the parent bank for Citizens Bank, "[w]as dubbed the 'hippie bank' for its community involvement, environmental programs and pioneering of ethical growth funds. While major banks were busy announcing profits, VanCity was handing profits back to its members—

Since the majority of Internet bank customers cannot visit a physical branch, they must contact the bank by telephone, email, postal service, fax, or some other more impersonal mechanism.[39] For persons accustomed to building a relationship with a personal banker, banking at an Internet bank is likely to lead to considerable frustration when problems arise.[40] This frustration may be aggravated when the Internet bank malfunctions and the limited number of customer service representatives are unavailable to help. One way to accommodate these types of customers is to open a physical brick and mortar branch. SFNB tried this approach in 1996.[41] Although operating a physical branch detracts from some of the uniqueness of an Internet bank, SFNB has attempted to maintain a technology-rich atmosphere at the branch.[42]

$9.3 million in 1995 alone." *Id.* Citizens Bank even offers a "Shared Interest VISA" card that has no annual or transaction fee and contributes 10 cents per transaction to a number of non-profit organizations. *See* Citizens Bank of Canada, *News and Views: Citizens Bank of Canada Launches "Visa Card With a Conscience"* (last modified Sept. 16, 1997) <http://www.citizensbank.ca/index10.html>. When the bank first received its charter from the Canadian Superintendent of Financial Institutions in February 1997, customers could only access their accounts through the bank's mainframe computer. *See id.* Since that time, Citizens Bank has launched a full service Internet bank offering checking and savings accounts, online mortgage applications, investment services, and a VISA credit card. *See* Citizens Bank of Canada, *Products and Services* (last modified Sept. 16, 1997) <http://www.citizensbank.ca/index4.html>.

39. *See* Jennifer Kingson Bloom, *Puzzler: What's CRA Duty of an On-Line Bank Banks, Regulators Ponder 'Reinvesting' in a Cyberspace 'Community,'* AM. BANKER, Jan. 7, 1997, at 18, *available in* 1997 WL 4746429.

40. Although the lack of a personal relationship with a banker poses a problem for some bank customers, people using an Internet bank are aware of the lack of human contact when they open accounts. Due to the rising number of people subscribing to the services of true Internet banks, this disadvantage is diminished by the increased convenience and ability to talk with a customer service representative on the telephone. *See* Eileen Ambrose, *New Bank To Let You Check Net On The Net — Indiana Is One Of The First States To Launch A Bank Where Members Receive Online Services*, THE INDIANAPOLIS STAR, Aug. 28, 1997, at CO1.

41. *See* Bloom, *supra* note 36, at 10A. When the bank began Internet operations, it also opened a physical branch in its original headquarters in Pineville, Kentucky. *See id.* The bank then opened an Atlanta branch which is now the home of the SFNB headquarters. *See id.* SFNB also plans to open branches in Palo Alto, California, and Cambridge, Massachusetts. *See Internet Banks Ramp Up Investment Programs*, BANK INV. PROD. NEWS, Feb. 3, 1997, *available in* 1997 WL 12150695; *see also* Stouffer, *supra* note 31, at E1 (stating that AIB also has an Atlanta office even though its main operations are in Columbia, South Carolina.)

42. *See* Bloom, *supra* note 36, at 10A. The branches have large video monitors to greet the customers, computer terminals with access to the Internet, web demonstration areas, and an ATM with smart card technology. *See id.* In addition, customer service representatives and loan officers are available to process personal and large retail loans, offer investment advice, sell travelers' checks, and rent safety deposit boxes. *See id.*

Another disadvantage of banking via the Internet is the limited means by which customers can make deposits. For instance, SFNB only accepts deposits by mail, credit card, wire transfer, or direct deposit.[43] Internet banks have attempted to comfort customers wary of these deposit mechanisms by providing toll-free access to customer service representatives who can verify deposit amounts.[44] The banks' websites also allow customers to confirm deposit and withdrawal activity.[45] Although designed for the computer-savvy customer, Internet banks have used physical branch openings and confirmation services to show customers that they are willing to adapt their services to match customer needs. Banks are aware of the cost savings and convenience of Internet banking, and therefore encourage increased customer familiarity with the Internet and online banking in order to contribute to the future growth of the newest form of electronic banking.[46]

---

43. *See* Security First Network Bank, *Customer Account Applications* (last modified June 18, 1997) <http://www.sfnb.com/apply/cusapp.html>. To make a deposit by credit card, customers may enter their credit card number on their screen as if they were making an Internet purchase. *See id.*

44. *See* Atlanta Internet Bank, *FAQ's (Frequently Asked Questions)* (last modified Aug. 11, 1997) <http://www.atlantabank.com/faq.htm#8>.

45. *See* Security First Network Bank, *Why Security First Network Bank* (last modified Aug. 12, 1997) <http://www.sfnb.com/whyus/index.html>. Customers have generally been very pleased with mail-in deposits. *See* Security First Network Bank, *SFNB-News Center-File Cabinet* (last modified Mar. 13, 1997) <http://www.sfnb.com/newscenter/customer comments.html>.

46. *See Australia: Cost Savings Drive Internet Banking*, EXCHANGE TELECOM. NEWSLETTER, Apr. 18, 1997, *available in* 1997 WL 10406481 (indicating that the Internet transactional costs, which are one-eighth the cost of traditional banking methods, are expected to contribute to a "four fold growth in Internet banking sites over the next three years"). At least two banks have already initiated procedures for establishing Internet banks. One such institution is First Internet Bank of Indiana, which plans to operate as a state bank. *See* Ambrose, *supra* note 40, at CO1; *see also Insurer to Offer Banking [:] Principal Mutual Life of Des Moines will open an Internet-based Savings and Loan as Part of Its Plan to Become a Full-Line Financial Service Provider Without Branches*, OMAHA WORLD-HERALD, Nov. 16, 1997, at 1M. In addition, CompuBank, the first national electronic bank, received a preliminary conditional charter from the Office of the Comptroller of the Currency (OCC) on August 20, 1997. *See* OCC, Application to Charter CompuBank, National Association, Houston Texas, Conditional Approval #253, (Aug. 20, 1997), *available in* 1997 WL 581004, 9 (O.C.C.). Initially, the bank plans to use modem access and a proprietary software program to meet the transaction needs of its customers. *See Capital Briefs: FDIC Approval for a Virtual National Bank*, AM. BANKER, Oct. 16, 1997, at 2 (noting that the FDIC granted Compubank's request for deposit insurance on October 14, 1997). In the future, CompuBank will add Internet access to its delivery channels. *See id.*

III. PROBLEMS WITH ELECTRONIC BANKING

Although electronic banking is convenient and cost-effective, the integration of new technology produces unique legal concerns. Although these concerns are numerous and complex, three of the most significant and troubling are security,[47] privacy,[48] and Community Reinvestment Act compliance.[49] Security and privacy concerns are not new, nor are they limited to online banking, web-based banking, or Internet banks. Similarly, CRA compliance is a concern for all banks, but Internet banks face unique difficulties.

A. Security

Despite the fact that millions of people are opening accounts and making deposits into Internet banks, one of the greatest barriers to increased web-based and online banking is a perceived lack of security.[50] In 1996, the media reported at least six successful attempts by hackers[51] to gain unauthorized access to information transmitted over the Internet.[52] Whether real or merely perceived, consumer concerns about security focus on hackers intercepting funds being transferred between accounts on the Internet and gaining

47. *See infra* notes 50-57 and accompanying text.

48. *See infra* notes 58-69 and accompanying text.

49. *See infra* notes 70-83 and accompanying text.

50. *See Electronic Banking: OTS Targets Security as the Greatest Area of Potential Risk to Thrifts in PC Banking*, 68 Banking Rep. (BNA) 1254 (1997).

51. A hacker is an individual who, through a series of random attempts or extensive mathematical calculation, breaks through the security walls of a company to gain access to confidential information. *See generally* Thomas W. Cashel, *Financial Services: Security, Privacy, and Encryption*, 3 B.U. J. SCI. & TECH. L. 4 (1997) (explaining how a security code can be broken by a hacker). Although the potential for hacking becomes greater as the number of electronic transactions increases, hackers have been breaking into computer systems for years. *See* Matt Barthel, *Bank Worker Gets Kudos for Cracking ATM Scam*, AM. BANKER, Oct. 25, 1993, at 24.

52. *See* Deborah Stokes, *PC Banking Slowly Overcomes Security Fears*, FIN. POST, Mar. 6, 1997, at E6. One example of hacking activity was the report that Kevin Mitnick "was accused of stealing 20,000 credit card numbers from Internet service provider Netcom ... [and] Carlos Felipe Salgado Jr. was indicted in May [1997] on charges that he stole 100,000 card numbers by tapping into the records of retailers who sell products on the Internet." *Bankers, Technology Experts Discuss How to Move Industry to Cyberspace*, DALLAS MORNING NEWS, Sept. 22, 1997, at 6D. *But see* Stouffer, *supra* note 31, at E1 (stating that AIB "says the chances of a hacker breaking into its system via a random guess of your very own password is one in one trillion") (emphasis added).

access to funds stored in bank accounts accessible through the Internet.[53] Although some apprehension is logical, some argue that the problem is more with perception than with reality.[54] One analyst argues that using a PC for banking services is safer than writing checks or using credit cards because a hacker would have to successfully invade layers of passwords and encryption on a computer to access the same information readily available on a paper check or a plastic card.[55] Even if a hacker invaded an account, he would only be able to request a wire transfer. Since a wire transfer could take days to process, Internet banks with top-notch security would have plenty of time to discover the unauthorized transaction.[56] Nevertheless, electronic banking consumers must live with the potential risks, though slight, that highly sensitive information could be disclosed to undesired third parties in an Internet transaction.[57]

---

53. *See generally* Eugene A. Ludwig, *Remarks at the Department of the Treasury Conference: Toward Electronic Money & Banking: The Role of Government*, Sept. 20, 1996 (visited Jan. 4, 1998) <http://www.occ.treas.gov/ftp/release/ 96-102.txt> (commenting that increased availability of information in a technological medium has caused greater public concern about "who has access to that [personal] information and how it is used").

54. *See* Newberry, *supra* note 5, at 94 (arguing that consumers merely perceive that security is a problem with Internet bank transactions even though the majority of these issues have already been resolved "from a technological standpoint"). One reporter has commented that buying things on the Internet is no riskier than transactions on the phone. *See* Mitch Wagner, *Conquering E-consumer Fears*, COMPUTERWORLD, Sept. 22, 1997, at 49R. Basically, it is no more a concern than "leaving your house with a pocketful of money." *Id.*

55. *See* Newberry, *supra* note 5, at 94; *see also* James T. Mulder, *Banking Without the Bank Online Banking Draws Customers Who Want Speed and Convenience*, POST-STANDARD, June 23, 1997, at C1; *see* Catherine A. Allen, Remarks on behalf of The Bankers Roundtable Banking Industry Technology Secretariat at the Consumer Electronic Payments Taskforce (July 17, 1997) (arguing that security concerns stem from consumer fear that credit card or bank account agreements might be breached) (unpublished manuscript, on file with the author).

56. *See* Mulder, *supra* note 55, at C1; *see also* Stouffer, *supra* note 31, at E1 (asserting that the Internet banks have assured their customers that banking on the Internet is "as secure as the gold at Fort Knox").

57. *See* Russell B. Stevenson, Jr., Statement at the Consumer Electronic Payments Task Force Public Meeting (July 17, 1997) (unpublished manuscript, on file with the author) ; *see also* Mulder, *supra* note 55, at C1 (stating that industry leaders admit that the Internet is not 100% fool-proof; and that no medium is safe all the time).

B. Privacy

While consumers' security concerns focus on protecting their account information from outsiders, their privacy concerns relate to preventing outsiders from tracing their steps on the Internet so that the outsider can create customer profiles for marketing purposes.[58] For example, when customers visit their bank's web site, various software programs use "clickstream" technology and "cookies" to track where customers visited before and after performing their bank transaction. A clickstream is an electronic trail that is captured by recording transactional information which allows the webmaster[59] at any site visited to determine the user's email address, what type of computer used, what was viewed at a site, how long the information was viewed, and which site was viewed before and after visiting that particular site.[60] Similarly, cookies "create a profile of your activities and store it in a text file that is placed on your computer's hard drive so that the next time you visit, the site will know better how to serve you."[61] These features allow banks to gain insight into consumer preferences on the Internet and better design their websites and services to suit those preferences. As with the three-dimensional world, banks may also use the information to compile lists to classify their market and target new customers.[62]

---

58. *See* Legal & Public Policy Committee of the Smart Card Forum, Inc., *Consumer Privacy and Smart Cards—A Challenge and an Opportunity*, presented at the Consumer Electronic Payments Task Force Meeting (June 9, 1997) (unpublished manuscript, on file with the author); *see also* Graphics, Visualization, and Usability Center, *GVU's Eighth User Survey Privacy Bulleted List* (last modified Jan. 12, 1998) <http://www.gvu.gatech.edu/user_surveys/survey-1997-10/bulleted/privacy_bullets.html> (stating that 66% of survey respondents do not register at web sites because they do not know how the information will be used, and 58% of the respondents do not trust the organization that is collecting the information).

59. A "webmaster" is the creator of a homepage or series of pages on the world wide web. *See Glossary of PC & Internet Terminology* (last modified Jan. 4, 1998) <http://homepages.enterprise.net/jenko/Glossary/GW.htm#WEBMASTER>.

60. *See* William S. Galkin, *Your Clickstream is Showing* (visited Feb. 27, 1998) <http://www.lawcircle.com/issue22.html>.

61. *Id.*; *see also DoubleClick, DoubleClick on Privacy* (last modifed Jan. 14, 1998) <http://www.doubleclick.net/general/onpriset.htm>.

62. *See* Joey Senat, *Why Does Someone Want That Information?* (last modified Apr. 25, 1997) <http://www.unc.edu/~jsenat/privacy/why.html>.

As consumers begin to realize how much personal information is available about them on the Internet,[63] they may become reluctant to engage in web-based banking transactions.[64] Most customers would assume that messages they send to a financial institution will only be accessible by the sender and the recipient. Although some electronic communications between financial institutions and customers are protected by contractual agreements and federal privacy statutes,[65] protection may not be absolute for all such communications.[66]

Unlike most electronic communications between banks and their customers, telephone communications frequently provide a warning that calls may be monitored for training or quality control purposes.[67] Similar warnings are rarely provided in electronic mail communications. As a result, information transmitted in an email message may be available to a wide range of bank officials or other unintended parties. In addition, customers often are not warned that electronic and voice communications with the bank may be saved in electronic storage for undisclosed periods of time.[68] The longer the communication is kept electronically, the greater the possibility of

63. *See supra* notes 60-61 and accompanying text.

64. *See* DigiCash, Interaction Privacy (visited July 15, 1997) <http://www.digicash.com/present/webversion/sld002.htm>.

65. *See infra* notes 125-130 and accompanying text.

66. Some companies and organizations that provide electronic mail to their employees specifically state that email transmitted on the company's email server may be viewed and/or stored by the organization. Accordingly, employees should be aware that anything they write on email is as open to the public as if they shared the information by word of mouth. *See, e.g.*, Electronic Rights and Responsibilities at UNC-Chapel Hill, Section IV: Privacy, Confidentiality, and Freedom of Expression (Aug. 29, 1994) (stating that the University archives digital communications like electronic mail, and system administrators have access to and will disclose the contents of those messages when contractual obligations, state law, or federal law requires them to do so).

67. *See*, e.g., Telephone interview with Customer Service Representative, First Union National Bank (Nov. 10, 1997) (stating that telephone calls are randomly monitored for security purposes). *But see* Netscape, *Security Information* (visited Oct. 20, 1997) <http://www.rocketmail.com> (containing a pop-up menu which states "[a]ny information you submit is insecure and could be observed by a third party while in transit . . . . If you are submitting passwords, credit card numbers, or other information you would like to keep private, it would be safer for you to cancel the transmission"). Although this message appears automatically at some secure websites, users do not always read the message and have the option to ignore the warning. *See id.*

68. *See supra* notes 66-67 and accompanying text.

misappropriation.[69] Thus, banks should consider setting limits on the amount of time they archive email messages.

C. CRA Compliance

Although security and privacy concerns are common to online banking, web-based banking, and Internet banks, compliance with the Community Reinvestment Act[70] (CRA) creates a unique problem for Internet banks. The CRA mandates that financial institutions insured by the Federal Deposit Insurance Corporation (FDIC) address and service the credit needs of the entire community in which they operate.[71] For a traditional bank, the community consists of the physical area where customers come to make deposits, apply for loans, and conduct other business transactions.[72] However, with an Internet bank, most of these transactions occur in cyberspace, thereby making the delineation of the appropriate community difficult.[73] Although Internet banks have been in operation since 1995, when making the latest revisions to the CRA in 1997, legislators did not address Internet banks or online banking.[74]

---

69. *See* Betty Ann Olmstead, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete*, DEF. COUNS. J., Oct. 1996, at 523.

> Each time the message is 'handled' by another server or personal computer, another copy is made. By the time the message reaches the recipient, several copies have been generated and stored. For each additional recipient of the e-mail message, the number of potential electronic copies of the document increases exponentially.

Id.

70. 12 U.S.C.A. § 2901-2907 (West Supp. 1997); 12 C.F.R. § 25.11(b)(1) (1998).

71. *See* Raymond E. Muth, *Activists are Challenging Bank Expansion on More Than CRA Performance*, 16 No. 3 BANKING POL'Y REP., Feb. 3, 1997, at 7.

72. *See id.* For example, a branch of First Union National Bank located in Chapel Hill, North Carolina, could define its "community" as Chapel Hill and develop programs which would target the credit needs of a University population as well as the upper, middle, and low-income residents of the town.

73. *See* Bloom, *supra* note 39, at 18.

74. *See* Muth, *supra* note 24, at 11. The adviser for external relations at the Office of the Comptroller of the Currency stated that at the time no bank had made such a significant stride into online or web-based banking as to require a review of compliance measures. *See id.* Instead, the latest CRA revisions generally stabilized the examination procedure, attempted to level the amount of training received by examiners, increased the amount of time for the examination process, and basically exempted small banks and thrifts from CRA requirements. *See* United States General Accounting Office, Community Reinvestment Act: Challenges Remain to Successfully Implement CRA, Nov. 1995, at 4.

Two of the Internet banks that maintain physical branches in Atlanta may have solved the community definition problem of CRA compliance.[75] SFNB, for example, receives deposits from all over the world via the Internet but concentrates its CRA efforts in the Atlanta community.[76] By opening a physical office in one area, this Internet bank can tailor its CRA compliance activities to the community where it physically operates and receives some of its deposits. With a focused plan such as SFNB's, Internet banks can address the credit needs of a specific physical community rather than attempting to serve the entire nation.[77] Since the majority of SFNB's customers and other Internet bank customers are affluent, well educated, and have higher than average median incomes,[78] SFNB's various CRA compliance activities in specific low-to-moderate income areas create a balance in the "entire" community served by the bank.[79]

---

75. *See supra* note 41 and accompanying text.

76. *See* Bloom, *supra* note 39, at 18. In contrast, AIB has not defined any specific CRA programs. *See id.* It did, however, specify that the 400,000 Internet users in the Atlanta area would be its target market. *See id.* Consequently, it seems that AIB directors could formulate more specific CRA compliance programs. *See Two New Internet Banks Come On-Line Internet*, BANK MARKETING INT'L, Mar. 1, 1996, at 2.

77. Many of the recent interpretive letters on CRA compliance address the needs of low to moderate income individuals and how banks interact with this sector of the American community. *See* Office of the Comptroller of the Currency, *CRA Interpretations* (last modified Jan. 27, 1998) <http://www.occ.treas.gov/cra/craintrp.htm>.

78. The Internet population has an average income of $66,700 per year; more than 80% have a college degree; and 75% are between the ages of 16 and 44. *See* AMERICA'S COMMUNITY BANKERS, *supra* note 22, at 17. Internet banking customers also carry an average balance of $20,000 in their certificate of deposit and money market accounts. *See id.* at 23; *see also* Bloom, *supra* note 39, at 18 (emphasizing the assertion of SFNB Chief Executive Officer, James S. "Chip" Mahan, that SFNB's customers are wealthier and more educated than the average bank customer). Individuals who engage in electronic banking generally fall between the ages of 35 and 45 and earn at least $150,000 annually per household. *See* Chambers, *supra* note 20, at G2.

79. Eugene Ludwig, the Comptroller of the Currency, has made a special effort in the past two years to ensure that all national banks comply with the CRA. *See Some Reforms Could Hurt CRA Programs*, REG. COMPLIANCE WATCH, Mar. 10, 1997, at 1. This past summer, he commented that despite the growth in electronic banking and the savings to financial institutions, "the new technologies give rise to potential access challenges for low- and moderate-income Americans" in that they must acquire personal computers and have bank accounts to take advantage of these new developments in the banking industry. Remarks by Eugene A. Ludwig, *Comptroller of the Currency, before the Women in Housing and Finance Technology Symposium, on Changes in the Financial Services Industry* (Dec. 4, 1996), 1 OCC Q.J. 114 (1997). In an era where banking practices have progressed to sole Internet based banks, it is surprising to note that "tens of millions of people in this country . . . are either unbanked or underbanked" for reasons ranging from

Despite the attempts by Internet banks to meet the banking needs of their local communities and thereby satisfy the CRA requirements, they do not serve large segments of low-to-moderate income communities because of their reliance on technology. Although the cost of personal computers (PC's) has decreased dramatically,[80] thirty percent of American households still do not own PC's, and many PC owners do not have access to the Internet.[81] It is quite likely, therefore, that many low-to-moderate income families are without either PC or Internet access.[82] Consequently, without strong efforts by Internet bank officers to find alternative ways to service lower income bank customers, this portion of the community may be excluded.[83]

IV. POSSIBLE SOLUTIONS TO THE SECURITY, PRIVACY, AND CRA COMPLIANCE PROBLEMS

Despite the problems associated with online banking, web-based banking, and Internet banks, industry leaders are working hard to formulate effective solutions. However, it is important to realize that it will take time to develop, accept, or implement any potential solutions. Designers and distributors of software and services that aim to reduce threats to secure transactions will be influential in addressing security and privacy concerns. In addition, the government may play a role in devising some solutions to these

---

distrust of the American banking system to inability to pay the service fees associated with obtaining and maintaining a basic checking or savings account. Donet D. Graves, "Access to Electronic Money and Banking for Consumers," Summary of Statement at the Consumer Electronic Payments Task Force Public Meeting (June 9, 1997), at 3 (unpublished manuscript, on file with the author).

80. *See* AMERICA'S COMMUNITY BANKERS, *supra* note 22, at 7.

81. *See id.* at 9.

82. *See* Wilson, *supra* note 1, at 688 One commentator states that:

> While there is great potential, if gone about in a careful and intelligent manner, the implications of electronic banking and technologies could pose a serious risk of further disenfranchising and excluding historically underserved communities. The lack of access to, as well as experience with computers, ATM's, and the like will limit their use by low-and moderate-income users.

Graves, *supra* note 79, at 4.

83. *See*, e.g., Bloom, *supra* note 39, at 18. In this article, Ms. Bloom refers to initial efforts of AIB officers to comply with the CRA, "[t]o be honest, we haven't spent a whole lot of time thinking about (CRA) . . . . The only CRA idea the bank has considered is posting public service announcements on its Web Site." *Id.*

problems. Finally, market participants themselves must agree to set standards and guidelines with which they will comply in order to diminish the problems associated with electronic banking. Working together, Internet industry members and government policy makers have the ability to greatly reduce security fears,[84] alleviate concerns about invasion of privacy,[85] and increase compliance with CRA principles.[86]

A. Security

1. Marketplace Initiatives

In response to the perceived and actual threats to the security of Internet transactions, members of the Internet commerce industry implemented several measures to eliminate threats to secure Internet transactions. Banks attempted to calm this fear with measures like the development of encryption and digital signatures,[87] smart cards,[88] firewalls,[89] and even biogenetic scanning.[90]

---

84. *See infra* notes 87-120 and accompanying text.

85. *See infra* notes 121-41 and accompanying text.

86. *See infra* notes 142-50 and accompanying text.

87. *See infra* notes 91-93 and accompanying text.

88. *See infra* notes 94-100 and accompanying text.

89. *See infra* notes 101-05 and accompanying text.

90. *See* Akweli Parker, *Norfolk Firm's Device Puts Banking At Your Fingertips*, VIRGINIAN-PILOT AND LEDGER-STAR, Sept. 5, 1997, at D1. An example of biogenetic technology is the LCI SmartPen which is a ball-pen with a built-in encryption system which allows authentication of an individual through the biometric characteristics of his signature. *See* Eric Vlietinck, *LCI Smart Pen* (last modified May 4, 1997) <http://www.thinck.com/smartpen.html>; *see also ATM Industry Eyes Biometrics: Technology Scans Characteristics of Iris to Verify Your Identity*, EVANSVILLE COURIER, June 7, 1997, at C5 (declaring that "'biometric identity' devices are being tested in automated teller machines as a substitute for plastic bank cards and personal identification numbers"). In the future, computer hardware designers could imbed biogenetic devices in keyboards or monitors so that an Internet bank customer could simply sit down at their computers, and the computer would automatically recognize their biogenetic characteristics. Advances like these could eliminate the need for personal identification numbers, ATM cards, tellers, or signatures to perform financial transactions, assuming state and federal governments grant equal legal force to these advances as a handwritten signature.

a. Encryption and Digital Signatures

Digital signatures can protect Internet transactions by using encryption to scramble a message.[91] Encryption is the process of disguising a message in order to hide its substance.[92] For example, application of a digital signature would change the text of a message that says, "Hello, my name is Adam" to "I#vfDKxLL%$&dkI12b,sdj&*(Sje." After a message or transaction is digitally signed, a certification authority issues a certificate that further authenticates the sender of the message.[93]

b. Smart Cards

Another way to secure information transmitted to an Internet bank is with a smart card.[94] A smart card contains an embedded chip which can record important information about the cardholder including: a social security number, bank information, blood type or a host of other information.[95] Although still in the developmental stages, smart card users may eventually authenticate Internet

---

91. *See* Thomas J. Smedinghoff, Presentation at the Consumer Electronic Payments Task Force Public Meeting (July 17, 1997) (unpublished manuscript, on file with the author); *see, e.g.*, Government Technology, *How to Sign on the Digital Line* (last modified July 17, 1997) <http://www. govtech.net/1995/gt/jun/features/elec.htm>.

92. *See* Smeddinghoff, *supra* note 91.

93. A certification authority is a trusted third party, typically a federal or state government entity, who verifies the identity of a person signing a message or electronic document digitally and confirms that the signature really belongs to the sender of the message. *See* Thomas J. Smedinghoff, *Digital Signatures: The Key to Secure Internet Commerce* 22 (unpublished manuscript, on file at McBride Baker & Coles, Chicago, Illinois). The certificate is an electronic record that documents the identity of the certification authority or other information. *See id.*

94. *See* Associated Press, *supra* note 52, at 6D. Smart cards also have the "capacity to encrypt, or scramble data that is transmitted to a business." *Id.*

95. Smart cards have been in use throughout the world since the early seventies. *See* ICone, *Quick History of Smart Cards* (last modified Feb. 12, 1998) <http://www.icone. com/bschau.htm#QH>. The first major pilot program in the United States occurred in the 1996 Atlanta Olympics, where First Union and NationsBank issued smart cards in varying denominations so that spectators at the Olympics could use a card for small purchases rather than carrying cash. *See generally A Southern Bank Goes It Alone Along The Atlanta Smart Card Trail*, DEBIT CARD NEWS, Oct. 30, 1997, *available in* 1997 WL 8934406. Other major pilot programs were in the testing phase in the Northeastern United States during the fourth quarter of 1997. *See* Mondex, *Mondex Pilots: New York* (last modified Mar. 1, 1998) <http://www.mondex.com/mondex/cgibin/printpage.pl?english+global&pilots/new york1.html>.

transactions by sliding their cards through smart card readers on computer keyboards.[96] Hewlett-Packard and other manufacturers have already designed a keyboard with a smart card reader.[97] This type of keyboard would allow customers to transfer funds between accounts or load additional funds onto their smart card without going to a bank or isolated smart card reader location.[98] However, the most significant problem with smart cards arises when an identifying smart card is lost or stolen.[99] Unless the card has built in security measures like a password or personal identification number (PIN), any person could potentially use the card to gain access to a bank account, leading to increased security threats. Consequently, if a bank issues smart cards to add security to the Internet access process, it should strongly and clearly encourage customers to safeguard their cards. The bank may also go further to implement procedures for recovery of funds in the event a smart card is lost or stolen.[100]

c. Firewalls

While the greatest security threat posed to online banking accounts may come from hackers, bank employees may also pose a threat to the security of these accounts.[101] A common procedure used to protect customer information from employees is the installation of firewalls which are security systems designed to protect customer

96. *See* Paul Lampru, VeriFone Introductory Comments at the Federal Trade Commission Meeting (July 17, 1997) (unpublished manuscript, on file with the author).

97. *See id.*

98. *See id.*

99. Some smart cards merely contain a chip which stores monetary value and no identifying information like date of birth, social security number, or biogenetic information. *See, e.g.,* First Union, VISA Cash (last modified Feb. 26, 1998) <http://www.firstunion.com/personal/visacash/>.

100. The EFTA limits consumer liability for lost cards and/or unauthorized fund transfers to fifty dollars. *See* 15 U.S.C. § 1693g(a)(1-2) (1994).

101. *See* Associated Press, *supra* note 53, at 6D. This article stated that:

> Companies willing to invest the time and money can create systems that are relatively secure from outside invaders .... Where most systems fall short ... is preventing theft from within ... "a lot of companies invest hundreds of thousands of dollars into a firewall [to prevent outsiders from accessing data]. Internally, they're wide open, ... [t]hey leave the corporate family jewels laying out on the table.

Id.

files from "viruses and unauthorized access" by bank employees.[102] The firewalls allow banks to "monitor and control Internet traffic coming into the site and keep [employees] from wandering to unauthorized areas."[103] Although banks admit that they monitor traffic at their web sites, this open admission of monitoring may be comforting to some customers and disheartening to others. While monitoring may be intended to prevent security breaches, it may also allow the website administrator to track customer behavior. Analysis of customer behavior may lead to questions about invasions of customer privacy even though the monitoring is done with the best interest of the customer's security in mind. For that reason, several national public interest organizations propose that banks limit access to private customer account information on a need-to-know basis.[104]

By conforming to well-integrated access procedures, including digital signatures, smart cards, and firewalls, consumers may feel more secure engaging in Internet banking transactions. These consumers will also know that banks took extreme measures to secure their web sites and the transactions therein from unintended third parties.[105]

---

102. Elliott C. McEntee, Statement on behalf of the National Automated Clearing House Association before the Consumer Electronic Payments Task Force (July 17, 1997) (unpublished manuscript, on file with the author) ; *see, e.g.,* Owensboro National Bank, *Internet Security* (last modified Feb. 23, 1997) <http://www.onb.abcbank.com/onb_scur.htm>. Owensboro National Bank uses the same operating system as the Department of Defense. *See id.* This system protects customer information and funds inside the bank. *See id.* "It uses multilevel technology and contains privilege and authorization mechanisms to control access to functions and commands. It also contains an audit mechanism which records logins and logouts, use of privilege, access violations and unsuccessful network connections. This allows for quick identification of any suspicious activity." *Id.*

103. Stokes, *supra* note 52, at E6.

104. *See* Marcia Sullivan, Testimony on behalf of the Consumer Bankers Association before the Consumer Electronic Payments Task Force (July 17, 1997) (unpublished manuscript, on file with the author).

105. For example, SFNB even advertises that its security system is the same one used by the Department of Defense. *See* SFNB, *SFNB-News Center-File Cabinet* (last modified Mar. 13, 1997) <http://www.sfnb.com/newscenter/security_issues.html>; SFNB, *Office of Thrift Supervision* (last modified Feb. 9, 1998) <http://www.sfnb.com/infodesk/bankinfo_ots.html> (stating that SFNB refused to become fully operational on the Internet despite its conditional approval from the OTS until it passed the regulator's hackerproof security requirements).

2. Government Initiatives

To bolster the security efforts of banks and other market participants, Congress passed the Electronic Funds Transfer Act (EFTA) in 1978.[106] The EFTA ensures that customers receive documentation of any funds transfers they initiate and limits customer liability when security measures are breached.[107] Each time a customer authorizes a transfer of funds, the bank must provide him with documentation of the transfer in "readily understandable language"[108] and in retainable form.[109] The disclosure statement is important because a wire transfer is an electronic exchange which typically does not involve a paper trail. However, the EFTA disclosure statement provides the customer with a retainable transfer receipt. As a security measure, customers may use this disclosure form as proof that they were the initiators of the transfer. Specifically, customers may rely upon this receipt as evidence that a funds transfer occurred.

Unfortunately, this receipt does not guarantee that unauthorized funds transfers will not occur. When the bank's security procedures fail, and a hacker breaks through to transfer funds from a customer's account, the EFTA limits the customer's

106. 15 U.S.C. §§ 1693-1693r (1994); Electronic Fund Transfers (Regulation E) 12 C.F.R. § 205.6(b). Regulation E defines electronic funds transfer as any transfer of funds "which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." 15 U.S.C.A. § 1693b; *see also* Niles S. Campbell, *Fed Proposes Stored-Value Card Rules; Regulation E to Cover New Technology,"* BNA BANKING DAILY, Mar. 21, 1996, at d4.

107. *See* 15 U.S.C.A. § 1693b. The purpose of EFTA is "to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems [but] ... [t]he primary objective of this title ... is the provision of individual consumer rights." *Id.*

108. *See id.* § 1693c. This disclosure statement must include several items: 1) the consumer's liability for the transfer; 2) the telephone number and address of the person to be notified if the transfer fails; 3) the type and nature of the transfer the consumer may initiate; 4) any charges for the transfers; 5) the consumer's right to stop payment of a preauthorized transfer; 6) the consumer's right to receive documentation of the transfer; 7) a summary of the error resolution provisions; 8) the financial institution's liability to the consumer; and 9) the circumstances under which the financial institution will release information about the consumer's account to a third party. *See id.*

109. *See* 12 C.F.R. § 205.4.

liability for the unauthorized transfer, given that the bank is notified of the breach within sixty days.[110]

In addition to the protections afforded in the EFTA, the proposed Article 2B of the Uniform Commercial Code (UCC) may provide a security feature for online banking relationships. Proposed Article 2B would cover "all licenses of information, as well as all contracts involving software."[111] Specifically, section 115 of the proposed Article requires parties to use an attribution procedure when engaging in the electronic exchange of information.[112] In an attribution agreement parties to the contract must agree on a method by which they will verify "that electronic authentication, records, messages, or performances are those of the respective parties. . . ."[113] This procedure would allow a bank to verify that a request to transfer or withdraw funds is a valid request from the purported customer rather than a fraudulent request from an unauthorized party.[114] If adopted, section 2B-115 of the UCC is likely to improve the security of online banking transactions.[115]

Along with the EFTA and the proposed Article 2B of the UCC, other legislative efforts focus on security and other aspects of electronic banking. For example, the National Conference of Commissioners on Uniform State Laws drafted a Uniform Electronic Transaction Act[116] which would, upon adoption, revise general

---

110. *See id.* at § 205.6(b)(1q)-(b)(3). The statute provides that consumers are liable for up to $50 for an unauthorized fund transfer given they notify the bank within 48 hours. *See id.* at § 205.6(b)(1). If the customer does not notify the bank within 60 days, he or she may be liable for up to $500. *See id.* at § 205.6(b)(2). Any time period beyond the 60 day notification period leaves the customer open to unlimited liability.

111. Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 974 (1997).

112. National Conference of Commissioners on Uniform State Laws, *November 1997 Draft: Section 2B-115: Attribution Procedure* (visited Nov. 25, 1997) <http://www.law.upenn.edu/bll/ulc/ucc2/2bnov97.htm>.

113. *Id.*

114. *See id.*

115. Although this section would appear to apply in large part only to online banking transactions because of the requirement of a proprietary software program, the drafters of this proposed section state that "Article 2B is not just a software contract statute." National Conference of Commissioners on Uniform State Laws, *February 1998 Draft: Introduction* (visited Mar. 1, 1998) <http://www.law.upenn.edu/bll/ulc/ucc2/2b298.htm>. Instead, the subject matter of Article 2B transactions lies in intangible information transactions which could include financial transactions on the Internet. *See id.*

116. *See* National Conference of Commissioners on Uniform State Laws, Nov. 25, 1997

contract law to accommodate emerging technologies in electronic banking and commerce.[117] Some states have also enacted laws which validate digital signatures.[118] Moreover, the United States House of Representatives introduced the Electronic Financial Services Efficiency Act of 1997[119] which would grant the same legal weight to "electronic authentication methodologies" as to written signatures.[120] Thus, both state and federal governments are working to ensure that the development of electronic banking is not delayed for security reasons. If market participants continue to communicate with legislators concerning the real security issues facing the industry, government efforts for reform will be more direct and have a greater impact on the electronic banking industry. This improved understanding between market participants and legislators will allow legislators to better regulate and set standards for secure financial transactions on the Internet.

B. Privacy

1. Marketplace Initiatives

Even though invasion of privacy concerns abound in the three-dimensional world, the surreptitious nature of privacy invasions on the Internet makes this concern even stronger in cyberspace. Internet marketers, however, appreciate the validity of privacy concerns and are developing products and services to ensure that Internet technology limits the invasion of consumer privacy. An example of a product designed to protect privacy is DoubleClick, a software program which develops target marketing strategies through anonymously assigned numbers rather than using technology[121]

Draft: Uniform Electronic Transactions Act (last modified Dec. 13, 1997) <http://www.law.upenn.edu/library/ulc/uecicta/eta1197.htm>.

117. *See* McBride, Baker & Coles, *Summary Of Electronic Commerce And Digital Signature Legislation: National Conference of Commissioners on Uniform State Law* (last modifed Dec. 7, 1997) <http://www.mbc.com/legis/nccusl.html>.

118. *See id.*

119. H.R. 2937, 105th (1997), *also available in* <http:www.house.gov/banking/11897bak.htm >.

120. *See id.*

121. *See supra* notes 60-61 and accompanying text.

which can identify Internet surfers.[122] A similar service is the Anonymizer which acts as a shield between the consumers and the web sites they visit so that the web site may not track the users to that page.[123] Other privacy protecting initiatives include the marketing and distribution of cookie management software and web browser options. These devices allow users to totally block advertising or to determine which cookies they want stored on their hard drives.[124] While these products may help Internet users protect their privacy interests, such products will only help those consumers who are aware that they exist or those customers who take the initiative to find other ways to protect their privacy.

2. Government Initiatives

To address this lack of awareness, federal and state governments could provide more education concerning privacy rights by increasing enforcement of existing privacy legislation and amending legislation to specifically address Internet privacy issues. For example, the Right to Financial Privacy Act[125] protects consumer privacy by prohibiting financial institutions from disclosing private financial information to the government unless the customer authorizes the disclosure or the information is required by a judicial summons or a search warrant.[126] Another example of existing legislation which addresses Internet privacy is the Fair Credit Reporting Act[127] which restricts disclosure of financial data by prohibiting the release of consumer report information except in the following situations: upon request of a court, upon receiving written instructions from the consumer or a person who intends to use the

122. *See* DoubleClick, *DoubleClick Int'l Home Page* (last modified Feb. 20, 1998) <http://www.doubleclick.net/>.

123. *See* Anonymizer, *The Handy Anonymizer Guide* (last modified Feb. 26, 1998) <http://www.anonymizer.com/surfing.html>.

124. *See* Joey Senat, *How Can You Hide the Information?* (last modified Apr. 25, 1997) <http://www.unc.edu/~jsenat/privacy/hide.html>. Netscape Navigator and the Microsoft Internet Explorer also contain options that will allow users to receive a warning before a cookie is stored on a hard drive. *See id.*

125. 12 U.S.C. §§ 3402-3403 (1994).

126. *See id.* at § 3402(1)-(5).

127. 15 U.S.C.A. § 1681b(a) (West Supp. 1997).

information in a specific business transaction, or upon a showing of another legitimate business need.[128]

Although the Right to Financial Privacy Act and the Fair Credit Reporting Act address consumer fears that hackers or government agencies will gain access to their financial data, neither statute expressly addresses the privacy of information transmitted over the Internet. Congress could amend these statutes to specifically cover information sent over the Internet or could draft new Internet privacy laws. One example of new legislation drafted to protect Internet privacy issues is the Electronic Communications Privacy Act[129] which prohibits anyone from intercepting email messages, from reading an intercepted email message when he or she is not the sender or intended recipient, and from gaining unauthorized access to messages stored in an archiving system.[130] Even though the statute prohibits interception and use of information in an email message, it does not appear to limit or preclude the use of other information (i.e. personal or financial data) transmitted on the Internet in marketing or other data collection activities.

3. Voluntary Regulations

Before drafting new legislation to protect electronic banking privacy interests, Congress should consider the voluntary initiatives taken by many industry groups to protect consumer privacy and avoid premature government legislation in this area. One such group is the Consumer Bankers Association (CBA) which aids Congress and bank regulators in forming regulations on electronic banking, privacy, and other retail banking issues.[131] Some of those guidelines require banks engaged in electronic banking to recognize the privacy interests of their customers and take steps to educate their employees

128. *See id.*

129. 18 U.S.C.A. § 2511(1) (West Supp. 1997).

130. *See id.*

131. *See* Sullivan, *supra* note 104; *see also* Legal & Public Policy Committee—Smart Card Forum Presentation at the Consumer Electronic Payments Task Force (July 17, 1997). Like the CBA, the Smart Card Forum recognizes a need to establish privacy guidelines to protect present and future users of smart cards at Internet banks and other Internet retail locations. *See id.*

about how to protect those customer interests.[132] The CBA believes that the government should allow self-regulation within the electronic banking community so the industry will be able to grow undisturbed.[133] Although the CBA supports self-regulation, it also supports government efforts to educate consumers about the risks involved in Internet transactions and possible safeguards to prevent disclosure of information to unintended third parties.[134]

The Banking Industry Technology Secretariat (BITS) section of the Bankers Roundtable, formed to promote and facilitate electronic banking, was also instrumental in devising industry-wide privacy guidelines.[135] Generally, their guidelines, like those of the CBA, encourage Internet market participants to recognize consumer privacy rights and limit the dissemination of personal information.[136] One potential provision includes a "Privacy Mark" that would enable consumers and industry players to be assured that the Internet banking service honors guidelines established in the industry.[137] In contrast to the CBA, BITS developed measures for the implementation and enforcement of privacy guidelines in the banking industry.[138]

Other groups working in this area include the National Information Infrastructure Working Group on Privacy,[139] the Federal

---

132. *See* Sullivan, *supra* note 104. Other guidelines include the following:

> [1] Limit the use, collection and retention of information about consumers to what is necessary to administer their accounts, provide superior service and offer consumers new opportunities; [2] Provide a means for consumers to remove their names from the company's telemarketing, online, mailing and other solicitation lists; . . . [3] Take appropriate disciplinary measures with employees who fail to adhere to such standards.

Id.

133. *See id.*

134. *See id.*; Susan Grant, Testimony on behalf of the National Consumers League, Remarks to the Consumer Electronic Payments Task Force (July 17, 1997) (stating that "[i]t is clear that a significant effort must be undertaken to educate the public, both consumers and businesses, about security and fair information practices in electronic commerce") (unpublished manuscript, on file with the author).

135. *See* Allen, *supra* note 55 and accompanying text.

136. *See id.*

137. *See id.*

138. *See id.*

139. *See* Edwin N. Lavergne & Rhonda S. VanLowe, *Online Privacy: What is the Law?* MULTIMEDIA L. REP., Apr. 1996, at 3. The National Information Infrastructure proposed privacy standards which would encourage companies using personal information to disclose

Trade Commission's Bureau of Consumer Protection Privacy Initiative,[140] and TRUSTe.[141] It is important that legislators consider the industry's efforts to resolve consumer privacy concerns without the aid of formal legislation. If the industry can adequately protect consumer privacy without government intervention, it will have more flexibility in adjusting its guidelines to future changes and developments in electronic banking. If the government becomes involved too early, this quickly evolving industry will have to slow down to adjust to the legislative process.

C. *CRA Compliance*

Unlike initiatives taken by the banking industry and the government to solve security and privacy problems, concern over CRA compliance may be best addressed by joint industry and government involvement. Because it is difficult to define the geographic community of an Internet bank, the bank could obtain classification as a "limited purpose bank" in order to comply with the CRA. A limited purpose bank only offers a "narrow product line (such as credit card or motor vehicle loans) to a regional or broader market."[142] Section 25.12(o) of the CRA permits limited purpose banks to establish means of fulfilling CRA lending requirements outside of direct consumer lending practices.[143] For example, a limited purpose Internet bank could meet its CRA requirement by making "personal computers available to low and moderate income ... individuals,"[144] seeking "qualified investment and community development service opportunities relating to providing computers

---

to the public how the information would be used. *See id.* These principles would not be enforceable but would serve as guidelines for industry participants. *See id.*

140. *See* Federal Trade Commission, *Workshop on Consumer Privacy on the Global Information Infrastructure* (last modified Sept. 15, 1997) <http://www.ftc.gov/bcp/privacy/privacy.htm>.

141. *See* TRUSTe, *Who Is TRUSTe?* (visited Mar. 1, 1998) <http://www.etrust.org/users/abouttruste.html> (establishing itself as an organization whose purpose is to foster an environment where consumers feel comfortable interacting with businesses on the Internet).

142. 12 C.F.R. § 25.12(o) (1997).

143. *See id.*

144. OCC, *supra* note 46, at 5 and accompanying text; *see also* 12 C.F.R. § 25.12 (n)(1)-(2) (1997) (defining "low income" as an "individual income that is less than 50 percent of the area median income" and "moderate income" as an individual income that is at least 50% and less than 80% of the area median income").

and computer literacy training through schools in [low-to-moderate income] areas,"[145] and investing in "credit counseling, small business incubation projects, . . . within the assessment area."[146] Although using the limited purpose bank classification offers an Internet bank a broader means of meeting a community's credit needs, the bank still faces the dilemma of defining its targeted *community*.[147]

To identify a relevant community for purposes of the act, Internet banks could establish a working definition of community for CRA purposes. Possible definitions include the region of the country where most depositors live, the region where the bank physically receives mail deposits, or even the region where the bank would like for its customer base to grow. If Internet banks, as a group, can determine how to define their geographic community, they may develop effective means to identify and serve the credit needs of their typical affluent customer,[148] as well as the low-to-moderate income individuals within that community.[149] Once Internet banks have agreed upon a definition for their geographic community, they could promote the greater objective of the CRA—to meet the credit needs of the entire community regardless of social or economic status.[150]

---

145. OCC, *supra* note 46, at 5.

146. *Id; see also* 12 C.F.R. § 25.41(b) (1997) (defining the assessment area for a limited purpose bank as "one or more MSAs [metropolitan statistical areas defined by the Director of the Office of Management and Budget] or one or more contiguous political divisions, such as counties, cities or towns, in which the bank has its main office, branches and deposit-taking ATMs").

147. If a bank were to select this option to meet its CRA requirements, it may also face the dilemma of having to limit its purpose to a narrow product line when itsmission may include an aggressive profit-making strategy which involves a broad range of products and services.

148. *See supra* note 78 and accompanying text.

149. *See, e.g.*, Bloom, *supra* note 39, at 18 (stating that "business by telephone, automated kiosk, or computer minimizes the possibility of racial or other discrimination"). This largely occurs because the process loses the interpersonal dynamic which can associate stereotypes and prejudices with various ethnic and social groups in American society. *See id.* Customers who apply for loans online through an Internet bank could avoid the sting of discrimination in the racially-biased setting of higher interest rates, shorter and more restrictive payment terms, or blatant denials of loans based on factors other than their ability to repay the loan in a timely fashion. However, the bank must ensure that the mathematical equations used in the software programs which determine the outcome of a loan application do not weigh these factors as imbedded information in a customer's electronic records (i.e. the race and gender of the person with social security number 123-45-6789 is a Hispanic female who lives in Beverly Hills, CA).

150. *See* 12 U.S.C.A. § 2901 (West Supp. 1997). Specifically, the stated purpose of the CRA is to ensure that the regulated financial institutions "serve the convenience and needs

V. CONCLUSION

Advances in computer technology are changing the way the world spends, invests, and accounts for money. Although only a small percentage of the world economy is currently taking advantage of electronic banking opportunities, that percentage will increase as people become more aware of technology and better educated about how to use it.[151] For example, with the rapid spread of technology-rich classrooms in the public education system, tremendous numbers of children will learn about the advantages the Internet offers. As these children mature, their reliance on computers and the Internet will help foster the growth of online banking, web-based banking, and Internet banks.

To remain competitive when the demand for electronic banking services increases, bank must maintain high standards of security and privacy. Industry leaders and government regulators have already begun the process of making Internet banking a safe and secure exercise with the development of security devices such as digital signatures, smart cards, firewalls,[152] Double-Click, and the Anonymizer.[153] As the demands of a more technology driven generation force banks into electronic banking, only those banks able to offer these and other security devices will survive.

Another key to the success of this industry is maintenance of the government's role as a cautious observer rather than as an active regulator.[154] The Internet changes constantly and so markedly that

---

of the communities in which they are chartered to do business." *Id.* at § 2901(a)(1). However, the statutory notes provide that the financial institutions must submit to their regulator a report comparing "residential, small business, and commercial lending activities . . . in low-income neighborhoods, minority, and distressed neighborhoods" with lending in other neighborhoods. *Id.* Along with this report, the institutions must submit reasons why there may be disparities in the lending practices and ways to mitigate those factors. *See id.*

151. *See* Grant, *supra* note 134 and accompanying text.

152. *See supra* notes 91-104 and accompanying text.

153. *See supra* notes 122-24 and accompanying text.

154. *See* Anason, *supra* note 37, at 4 (quoting OTS Director, Nicolas Retsinas, "'[r]egulators should not impede the progress of technology, but must be cognizant of the importance of protecting the depositors and users of Internet banking systems'"). The Comptroller of the Currency even stated that regulating Internet commerce and banking at this time runs "the risk of killing the golden goose before it lays any eggs." Dean Anason, *Regulating E-Commerce: Damned If You Do . . .*, AM. BANKER, June 20, 1997, at 3. Deputy Treasury Secretary, Lawrence H. Summers, also believes that no regulations have

significant government intervention may slow down or halt its progress.[155] In contrast, self-imposed industry guidelines could be easily altered to rapidly keep pace with emerging Internet developments. However, government regulators should stay abreast of any developments so that they will be informed if regulation becomes necessary in the future. While the government observes this new phenomenon, electronic banking industry leaders must continue to develop new ways to make electronic banking a more efficient and secure alternative for the next generation.

KIMBRELLY KEGLER

been introduced about Internet commerce because "policy makers have not wanted to introduce preemptive regulations." *Id.*

155. *But see* Wilson, *supra* note 1, at 794 (suggesting that regulation implemented now could also prevent "expensive corrective action in the future"); Anason, *supra* note 154, at 3 (reporting that some legislators feel that something should be done now to prevent possible embarrassment in the case where a hacker makes a "major score").